# Distributed Security Architectures
## *"Providing Authorization for Distributed Resources"*

Mary R. Thompson [*], Lawrence Berkeley National Laboratory
Abedilah Essiari, Lawrence Berkeley National Laboratory
Keith Beattie, Lawrence Berkeley National Laboratory

*Summary*

*The overall goal of this project is to provide assured, policy-based access control for computer-mediated resources in wide-area-network environments. The intended resource domains include Web/Grid Services, data or services accessed via Web servers, standalone distributed applications and on-line collaborations. We have implemented a practical, general solution for policy-based access control. Our next step is to adapt our software to the emerging standards for Grid authorization while keeping our current distributed policy model.*

## 1. Introduction

The Distributed Security Architectures project is researching and implementing practical, general solutions for authorization of access to distributed resources, such as Web/Grid services, data or services accessed via Web servers, standalone distributed applications and on-line collaborations.

Our work is motivated by the increasing dependency of scientists on distributed systems for their applications and interactions. The earlier model of large server sites supporting a group of users has been supplemented by peer-to-peer collaborations between people, and light-weight, interoperable commodity services. Many of these systems started out requiring little or no authentication or authorization, but as scientists start to depend on them to control valuable resources, authentication and authorization are demanded.

## 2. Approach: Certificate-based policy

We have implemented and deployed a modular authorization service, called Akenti, that uses a requestor's authenticated X.509 identity certificate and a set of signed policy documents describing the resource's access policy in order to determine access.

These policy documents can be created and maintained by multiple stakeholders for the resource, and can be stored independent of the resource-server platform. Thus a common policy for resources that span multiple servers can be used to facilitate centralized control. Alternatively, a policy can be created by local stakeholders and apply only to local resources, thereby allowing local control. Since multiple stakeholders and distributed policies are allowed, a resource domain can choose its preferred mix of local and central control.
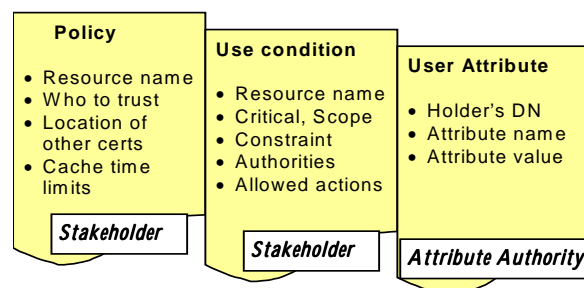


*Figure 1. Akenti policy certificates*

These documents are written in XML (Extensible Markup Language, which provides self-descriptive tags for each item) in order to be both conveniently machine

parseable and readily understood by resource stakeholders. We provide both a command-line interface to sign an XML document and a menu driven graphical interface to create and sign them.

## 3. Impact on Science

We have worked closely with the SciDAC National Fusion Collaboratory to use the Akenti authorization server to protect resources on the Fusion Grid. The Fusion Grid provides remote access to fusion data repositories and compute servers which run one of the commonly used fusion analysis codes, TRANSP.

Within the collaboratory the LBNL and ANL researchers integrated the Globus job-manager with Akenti, in order to provide fine-grained job authorization. In normal Globus job submission, the requestor is granted the equivalent of a user login to the machine. In practice that means that he can call the job-manager to execute any binary on the machine or to upload his own code to execute. In addition to starting new jobs, a Globus remote user can query, suspend or kill the jobs that he previously started.

The Fusion Grid wanted to limit the code that could be executed to only TRANSP code. At the same time, they wanted to expand the rights of some administrative users to be able to suspend or kill jobs started by people other than themselves.

After testing an early prototype Globus-Akenti integration that only restricted which programs could be executed, we worked with the ANL job-manager developers to design callouts from the job-manager that allow for authorization for both starting and managing jobs. We provide a plug-in module that parses the security context information from the job-manager and calls the Akenti authorization libraries to make an access decision. It is our intention that these pieces can be used by other SciDAC Grids

to provide fine-grained job control. The Akenti plug-in module can be used as delivered or can act as a model to integrate other authorization schemes with the job-manager.

We are also working with the scalable peer-to-peer information sharing project (SciShare) to provide Akenti authorization for file sharing. In the peer-to-peer environment, distributed signed policy helps to prevent an unwanted dependency on a central authorization server.

Akenti is also being used by the NSF NIMI (National Internet Measurement Infrastructure) project to provide access control for uploading and executing monitoring tools at distributed sites.

This work's main contribution to the DOE Science mission is to provide a pluggable authorization service to facilitate the secure sharing of resources in collaboratories or Grids. Akenti's model of stakeholder control over resources encourages scientists to share resources with their colleagues.

Our next step is to standardize clearly defined interfaces between access enforcement points and authorization services such as we used in the Akenti - Globus integration. We are working with the Global Grid Forum OGSA Authorization WG on developing standard protocols for authorization queries and responses. As soon as these standards are complete, Akenti will be modified to use them in order to be callable from the Grid Service version of the Globus job-manager.

**For further information on this subject contact:**

Mary R. Thompson
Computational Research Division
Lawrence Berkeley National Laboratory
Berkeley, CA 94720

Phone: 510-486-7408
E-mail: mrthompson@lbl.gov